UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,974	12/05/2001	Royce E. Slick	36.P327	9396

5514 7590 01/24/2006

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/010,974	SLICK ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 October 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/7/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed October 6, 2005, have been fully considered but they are not persuasive.

2. Claims 1-5 and 7-34 are pending and have been examined.

Response to Amendment

3. The objections to the specification and to the abstract are withdrawn.

4. The rejection of claim 27 under 35 USC § 112 is withdrawn.

5. Claim 34 is rejected under 35 U.S.C. 102(e) as being anticipated by **Currans** (US Patent 6,971,007). Claims 1-2, 5, 7-15, 19-21, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wiegley** (US Patent Number: 6,711,677). Claims 3-4, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wiegley**, and further in view of **Lohstroh** et al. (US Patent Number: 5,953,419, hereinafter **Lohstroh**). Claims 16-18, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wiegley**, and further in view of **Langford** et al. (US Patent Number: 6,470,450, hereinafter **Langford**). Claims 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wiegley**, and further in view of **Lohstroh** and **Langford**. Claims 28, 30, 31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wiegley**, and further in view of **Young** et al. (US Patent Number: 6,473,508, hereinafter **Young**). Claims 29 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Wiegley** and **Young**, and further in view of **Langford**.

6. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically

pointing out how the language of the claims patentably distinguishes them from the references.

7. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

8. The instant application merely makes use of conventional and well-known techniques for authentication and verification of parties involved in a communications system. The instant application replaces one party of a traditional public key encryption exchange with a printer. Under this scenario, Alice and Bob (Bob being the printer) securely communicate using public key encryption. Public key encryption also provides, as it is well known to someone of ordinary skill in the art, means to verify a message or a key haven not been tampered with. These information security concepts are clearly taught by Galasso et al. (US Patent 6,148,387) on columns 19-23, the main difference between Galasso et al. and the present claimed invention is that the instant application is directed towards exchanges between an information processing apparatus and an image forming apparatus.

9. Furthermore, it was conventional and well known for Alice (a party to a communications session) to verify Bob's (a second party to the communications session) key prior to using Bob's key to encrypt content to be sent to Bob. In the instant application, the information processing apparatus of claim 34 plays the role of Alice and

the image forming apparatus plays the role of Bob in a traditional public key encryption scenario.

10. Assuming arguendo the Prior Art does not, in any way, teach or suggest, **to someone of ordinary skill in the art**, "receiving a target public key corresponding to a target device; obtaining a user-specific key pair from a secure registry; using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key; storing the target key verifier and the target public key in a storage area; retrieving the target key verifier and the target public key from the storage area; applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key; and encrypting data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device", at the very least, Wiegley provides the base architecture, including public/private key architecture and hash functions to verify data, for someone of ordinary skill in the art to build upon.

Drawings

11. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "**92**" has been used to designate both "**decryption algorithm**" and "**encryption algorithm**" (amended fig 7). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claim 34 is rejected under 35 U.S.C. 102(e) as being anticipated by Currans.

Regarding claim 34, Currans teaches an information processing apparatus which transmits data to an image forming apparatus comprising: storing means configured for storing a public key in a secure area (column 4, lines 1-67); generation means configured for generating verification information from the public key (column 4, lines 1-67); obtaining means configured for obtaining the public key from the image forming apparatus (column 4, lines 1-67); verification means configured for verifying whether or not the public key obtained by the obtaining means is modified from the public key stored in the secure area by the storing means (column 4, lines 1-67); and encryption means configured for, at the time of the encryption, using the public key obtained by the obtaining means (column 6, lines 1-67), when the verification means verifies that the public key obtained by the obtaining means is not modified from the public key stored in the secure area by the storing means and not using the public key

obtained by the obtaining means when the verification means verifies that the public key obtained by obtaining means is modified from the public key stored in the secure area by the storing means (column 3, lines 1-67, column 4, lines 1-67, column 5, lines 1-67, column 6, lines 1-67).

Claim Rejections - 35 USC § 103

14. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15. Claims 1-2, 5, 7-15, 19-21, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley.

Regarding claim 1, Wiegley teaches a receiving step of receiving a target public key corresponding to a target device (column 4, lines 30-35); an obtaining step of obtaining a user-specific key pair from a secure registry (column 4, lines 47-65); a key encrypting step of using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key (column 4, lines 47-65); a storing step of storing the target key verifier and the target public key in a storage area (column 4, lines 47-65); a retrieving step of retrieving the target key verifier and the target public key from the storage area (column 5, lines 4-15); a verification step of applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key (column 4, lines 47-65). Wiegley teaches a data-encrypting step of encrypting data (column 4, lines 57-60) using a session key, and encrypting the session key using the printer's public key (column 4, lines 52-55). Wiegley does not expressly disclose a data encrypting step of encrypting

data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the data using the printer's public key. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to said receiver.

Regarding claim 2, Wiegley does not expressly disclose wherein the user-specific key pair is obtained from a key function call which is supported by an operating system executing in the computing device. However, Examiner takes Official Notice that the use of function calls supported by an operating system is conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a key function call which is supported by an operating system executing in the computing device since Examiner takes Official Notice that the use of function calls supported by an operating system is conventional and well known.

Regarding claim 5, Wiegley does not expressly disclose creating an encrypted version of the target public key. Wiegley does teach receiving the public key and a session identifier, and creating an encrypted version of the session key (column 4, lines 30-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the target public key instead of the session key identifier. One of ordinary skill in the art would have been motivated to do so

because it was well known in the art to use a receiver's public key to encrypt a message destined to said receiver.

Regarding claim 7, Wiegley teaches wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm (column 5, lines 4-24).

Regarding claim 8, Wiegley teaches wherein the verification step further includes using a key verification algorithm to compare the decrypted target key verifier to the target public key for verifying the authenticity of the target public key (column 5, lines 4-24).

Regarding claim 9, Wiegley does not expressly disclose wherein the verification step is performed by a verification function call which is supported by an operating system executing in the computing device. However, Examiner takes Official Notice that the use of function calls supported by an operating system is conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a verification function call which is supported by an operating system executing in the computing device since Examiner takes Official Notice that the use of function calls supported by an operating system is conventional and well known.

Regarding claim 10, Wiegley does not expressly disclose wherein the target key verifier created in the key encrypting step is a digital signature of the target public key. However, Wiegley teaches computing a hash value for the session key and the session identifier and encrypting it using the printer's public key (column 5, lines 48-67, column

6, lines 1-50). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compute a hash value or digital signature. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use digital signatures for providing assurance that there has been no modification of a message since it was digitally signed.

Regarding claim 11, Wiegley does not expressly disclose wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then encrypting the target key hash with the user-specific private key using an encryption algorithm. However, Wiegley teaches computing a hash value for the session key and the session identifier and encrypting it using the printer's public key (column 5, lines 55-62). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compute a hash value and encrypting it. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use digital signatures for providing assurance that there has been no modification of a message since it was digitally signed.

Regarding claim 12, Wiegley does not expressly disclose wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then subjecting the target key hash to a security algorithm. However, Wiegley teaches computing a hash value for the session key and the session identifier and encrypting it using the printer's public key (column 5, lines 55-62). Therefore, it would have been obvious to one having ordinary skill in the

art at the time the invention was made to compute a hash value and encrypting it. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use digital signatures for providing assurance that there has been no modification of a message since it was digitally signed.

Regarding claim 13, Wiegley teaches wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm to obtain a decrypted target key hash (column 6, lines 14-27).

Regarding claim 14, Wiegley does not expressly disclose wherein the verification step further includes reapplying a hashing algorithm to the target public key to obtain a new target key hash and using a hash verification algorithm to compare the decrypted target key hash to the new target key hash for verifying the authenticity of the target public key. However, Wiegley teaches computing a hash value for the session key and the session identifier, decrypting the hash value received, and comparing the values (column 6, lines 14-27). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to reapply a hashing algorithm to the target key and to verify the hash value by comparing the decrypted hash to the new hash value. One of ordinary skill in the art would have been motivated to do so to further verify authenticity of the data received.

Regarding claim 15, Wiegley does not expressly disclose wherein the verification step is performed by a verification function call which is supported by an operating system executing in the computing device. However, Examiner takes Official Notice that the use of function calls supported by an operating system is conventional

and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a verification function call which is supported by an operating system executing in the computing device since Examiner takes Official Notice that the use of function calls supported by an operating system is conventional and well known.

Regarding claim 19, Wiegley teaches wherein the target device is a printer (column 4, lines 30-45). Wiegley does not expressly disclose that the target public key is a printer public key. However, Wiegley does teach sending a session identifier and the printer public key to the device. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the printer public key instead of the session identifier. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to said receiver.

Regarding claim 20, Wiegley teaches wherein, in the receiving step, the printer public key is received in response to a key request sent to the printer (column 3, lines 62-67, column 4, lines 1-20).

Regarding claim 21, Wiegley teaches wherein the method is performed in a printer driver executing on the computing device (column 3, lines 40-56).

Regarding claim 27, Wiegley teach an information apparatus which transmits encrypted data to a target device, the information apparatus securely storing a public key for encryption of the data and utilizing a user-specific key pair which is securely stored in the apparatus, comprising: receiving means for receiving a target public key

corresponding to a target device (column 4, lines 30-35); obtaining means for obtaining a user-specific key pair from a secure registry (column 4, lines 47-65); key encrypting means for using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key (column 4, lines 47-65); storing means for storing the target key verifier and the target public key (column 4, lines 47-65); retrieving means for retrieving the target key verifier and the target public key from the storing means (column 5, lines 4-15); verification means for applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key (column 4, lines 47-65). Wiegley teaches a data-encrypting step of encrypting data (column 4, lines 57-60) using a session key, and encrypting the session key using the printer's public key (column 4, lines 52-55). Wiegley does not expressly disclose data encrypting means for encrypting data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the data using the printer's public key. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to said receiver.

16. Claims 3-4, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley, and further in view of Lohstroh.

Regarding claim 3, Wiegley does not expressly disclose wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the

computing device. However, Lohstroh et al. teach wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the computing device (column 23, lines 57-67, column 24, lines 1-11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have the operating system maintain a key-pair associated with each user. One of ordinary skill in the art would have been motivated to do so to further control access to secure data (Lohstroh et al., column 4, lines 1-15).

Regarding claim 4, the combination of Wiegley and Lohstroh et al. teaches the limitations as set forth under claim 3 above. Furthermore, Lohstroh et al. teach wherein each user-specific key pair can only be accessed by providing the operating system with user identification data corresponding to the user-specific key pair (column 23, lines 57-67, column 24, lines 1-11).

Regarding claim 22, Wiegley teaches a receiving step of receiving a printer public key corresponding to a printer (column 4, lines 30-35); a first hashing step of applying a hashing algorithm to the printer public key to create a first printer key hash (column 5, lines 48-67, column 6, lines 1-50); an encryption step of applying an encryption algorithm to encrypt the first printer key hash with a user-specific private key from the user-specific key pair, thereby creating a printer key signature (column 5, lines 48-67, column 6, lines 1-50); a storing step of storing the printer key signature and the printer public key in a storage area (column 4, lines 47-65); a retrieving step of retrieving the printer key signature and the printer public key from the storage area (column 5, lines 4-15); a second hashing step of applying the hashing algorithm to the retrieved

printer public key to create a second printer key hash (column 6, lines 14-27); a decrypting step of applying a decryption algorithm to decrypt the printer key signature with a user-specific public key from the user-specific key pair, thereby retrieving the first printer key hash; a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the retrieved printer public key (column 6, lines 14-27). Wiegley teaches a data-encrypting step of encrypting data (column 4, lines 57-60) using a session key, and encrypting the session key using the printer's public key (column 4, lines 52-55). Wiegley does not expressly disclose a print data encrypting step of applying an encryption algorithm to print data using the retrieved printer public key, in the case that the authenticity of the retrieved printer public key is verified, to create encrypted print data for transmission to the printer; nor an obtaining step of obtaining a user-specific key pair from a secure registry upon receipt of a corresponding user identification. However, Lohstroh et al. teach an obtaining step of obtaining a user-specific key pair from a secure registry upon receipt of a corresponding user identification (column 23, lines 57-67, column 24, lines 1-11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the data using the printer's public key. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to said receiver.

17. Claims 16-18 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley, and further in view of Langford.

Regarding claim 16, Wiegley does not expressly disclose wherein the receiving step includes applying a hashing algorithm to the received target public key to obtain a received target key hash and using a hash verification algorithm to compare the received target key hash to a test target key hash for verifying the authenticity of the received target public key. However, Langford teaches a system that provides a computed hash value to an output interface and receives a response through an input interface, such as a keyboard (column 7, lines 50-67, column 8, lines 1-20) for a user to compare the displayed hash value to a trusted hash value. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compare a computed hash value of received data to a trusted hash value for verifying the authenticity of the received value. One of ordinary skill in the art would have been motivated to do so because it is well known in the art to verify authenticity of received data by using hash values (Langford, column 7, lines 60-67, column 8, lines 1-20).

Regarding claim 17, the combination of Wiegley and Langford teaches the limitations as set forth under claim 16 above. Furthermore, Langford teaches wherein the test target key hash is input by a user (column 7, lines 50-67, column 8, lines 1-20).

Regarding claim 18, the combination of Wiegley and Langford teaches the limitations as set forth under claim 17 above. Furthermore, the combination of Wiegley and Langford teaches wherein the target device is a printer (Wiegley, column 4, lines 30-45) and wherein the test target key hash is obtained from a test page printed by the printer (Langford, column 7, lines 56-60, a printer is a well known output interface).

Regarding claims 23, Wiegley teaches a first receiving step of receiving in the computing device a printer public key corresponding to a printer (column 4, lines 30-35); a hashing step of applying a hashing algorithm to the printer public key to create a first printer key hash (column 5, lines 48-67, column 6, lines 1-50); and a storing step of storing, in the case that the authenticity of the received printer public key is verified in the verification step, the received printer public key in a memory area of the computing device (column 4, lines 30-46). Wiegley does not expressly disclose a second receiving step of receiving in the computing device a predetermined second printer key hash obtained from a test page printed by the printer, wherein the second printer key hash is input into the computing device by a user-input means connected to the computing device; a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the received printer public key. However, Langford et al. teach a second receiving step of receiving in the computing device a predetermined second printer key hash obtained from a test page printed by the printer, wherein the second printer key hash is input into the computing device by a user-input means connected to the computing device (column 7, lines 50-67, column 8, lines 1-20); a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the received printer public key (column 7, lines 50-67, column 8, lines 1-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compare a computed hash value of received data to a trusted hash value for verifying the authenticity of the received value. One of ordinary

skill in the art would have been motivated to do so because it is well known in the art to verify authenticity of received data by using hash values (Langford et al., column 7, lines 60-67, column 8, lines 1-20).

18. Claims 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley, and further in view of Lohstroh and Langford.

Regarding claims 24, the combination of Wiegley, Lohstroh et al., and Langford et al. teaches the limitations as set forth under claims 1-23 above. Furthermore, the combination of Wiegley, Lohstroh et al., and Langford et al. teaches computer readable medium a program memory for storing process steps executable to perform a method according to any of claims 1 to 23; and a processor for executing the process steps stored in said program memory (Wiegley, column 4, lines 1-67).

Regarding claims 25, the combination of Wiegley, Lohstroh et al., and Langford et al. teaches the limitations as set forth under claims 1-23 above. Furthermore, the combination of Wiegley, Lohstroh et al., and Langford et al. teaches process steps executable to perform a method according to any of claims 1 to 23 (Wiegley, column 4, lines 1-67).

Regarding claims 26, the combination of Wiegley, Lohstroh et al., and Langford et al. teaches the limitations as set forth under claims 1-23 above. Furthermore, the combination of Wiegley, Lohstroh et al., and Langford et al. teaches computer-executable process steps comprising process steps executable to perform a method according to any of claims 1 to 23 (Wiegley, column 4, lines 1-67).

19. Claims 28, 30, 31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley, and further in view of Young.

Regarding claim 28, Wiegley teaches an information apparatus which transfers encrypted print data to a printer, the apparatus comprising: retrieving means for retrieving a public key from said printer (column 3, lines 62-67, column 4, lines 30-35); generating means for generating verification information from the public key (column 5, lines 48-67, column 6, lines 1-50); recognizing means for recognizing a printing instruction (column 2, lines 40-56). Wiegley does not disclose expressly verification means for verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key; and control means for controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the retrieved public key is verified as changed. However, Young et al. teach verification means for verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key (column 9, lines 22-36); and control means for controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the retrieved public key is verified as changed (column 9, lines 22-36). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the public key of a sender at a receiving end (the printer sending its public key to the information apparatus) and based on this verification process, proceed accordingly (encrypt data and send it to the printer). One of ordinary

skill in the art would have been motivated to do so because it was well known in the art to verify the authenticity of a received message (Young et al., column 9, lines 32-36).

Regarding claim 30, the combination of Wiegley and Young et al. teaches the limitations as set forth under claim 28 above. Furthermore, Young et al. teach wherein said control means controls the encryption processing to encrypt the print data by using a user specific key obtained by an obtaining means and to encrypt the user specific key by using the public key (column 9, lines 22-36).

Regarding claim 31, Wiegley teaches an information processing method for transferring encrypted print data to a printer, the method comprising: a retrieving step of retrieving a public key from said printer (column 3, lines 62-67, column 4, lines 30-35); a generating step of generating verification information from the public key (column 5, lines 48-67, column 6, lines 1-50); a recognizing step of recognizing a printing instruction (column 2, lines 40-56). Wiegley does not disclose expressly a verification step of verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key; and a control step of controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the retrieved public key is verified as changed. However, Young et al. teach a verification step of verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key (column 9, lines 22-36); and a control step of controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the

retrieved public key is verified as changed (column 9, lines 22-36). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the public key of a sender at a receiving end (the printer sending its public key to the information apparatus) and based on this verification process, proceed accordingly (encrypt data and send it to the printer). One of ordinary skill in the art would have been motivated to do so because it was well known in the art to verify the authenticity of a received message (Young et al., column 9, lines 32-36).

Regarding claim 33, the combination of Wiegley and Young et al. teaches the limitations as set forth under claim 31 above. Furthermore, Young et al. teach wherein said control step controls the encryption processing to encrypt the print data by using a user specific key obtained by an obtaining step and to encrypt the user specific key by using the public key (column 9, lines 22-36).

20. Claims 29 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley and Young, and further in view of Langford.

Regarding claim 29, the combination of Wiegley and Young et al. does not expressly disclose obtaining means for obtaining a user specific key stored in a computer; input means for inputting authentication information; and determining means for determining whether to allow the obtaining means to obtain the user specific key. However, Langford et al. teach obtaining means for obtaining a user specific key stored in a computer (column 5, lines 56-67, column 6, lines 1-29); input means for inputting authentication information (column 5, lines 56-67, column 6, lines 1-29); and determining means for determining whether to allow the obtaining means to obtain the

user specific key (column 5, lines 56-67, column 6, lines 1-29). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate user access to a user specific key. One of ordinary skill in the art would have been motivated to do so to protect user information (Langford et al., column 1, lines 35-65).

Regarding claim 32, the combination of Wiegley and Young et al. does not expressly disclose an obtaining step of obtaining a user specific key stored in a computer; an input step of inputting authentication information; and a determining step of determining whether to allow the obtaining step to obtain the user specific key. However, Langford et al. teach an obtaining step of obtaining a user specific key stored in a computer (column 5, lines 56-67, column 6, lines 1-29); an input step of inputting authentication information (column 5, lines 56-67, column 6, lines 1-29); and a determining step of determining whether to allow the obtaining step to obtain the user specific key (column 5, lines 56-67, column 6, lines 1-29). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate user access to a user specific key. One of ordinary skill in the art would have been motivated to do so to protect user information (Langford et al., column 1, lines 35-65).

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Lee (US Patent 6,628,413) teaches a JAVA printer using any available security technique (columns 3-6). Lloyd (US Patent Application Publication 2003/0014640) teaches a printer using public key encryption and hash functions to verify information in transit has not been tampered with (paragraphs 20-30). Wu et al. (US Patent Application Publication 2002/0042884) teaches a printer, digital certificate, hash functions, and public key encryption for providing a secure printing environment, authenticating a printer, etc. (pages 7-13). Takaragi et al. (US Patent 6,370,247) teaches using hash values and encryption for data protection (columns 5-6). Fischer (US Patent 5,005,200) teaches a public key/digital signature system. Debry (US Patent 6,918,042) teaches a printer storing a key and a certificate authority also storing said key

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

23. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100